Chapter Twelve

THE ADVENT OF NETWAR*

John Arquilla and David Ronfeldt

CONCEPTUAL OUTLINES

In our view, the information-age conflict spectrum looks like this: What we term "cyberwar" will be an ever-more-important entry at the military end, where the language is normally about high-intensity conflict (HIC) and middle-range conflict (MRC). "Netwar" will figure increasingly at the societal end, where the language is normally about low-intensity conflict (LIC) and operations other than war (OOTW—a broader concept than LIC that includes peacekeeping and humanitarian relief operations). Whereas cyberwar will usually see formal military forces pitted against each other, netwar is more likely to involve nonstate, paramilitary, and other irregular forces. Both concepts are consistent with the views of analysts like Van Creveld (1991) who believe that a transformation of war is under way, leading to increased "irregularization."

The terms above reflect two assumptions (or propositions) about the information revolution. One is that conflicts will increasingly depend on, and revolve around, information and communications—"cyber"-matters, broadly defined. Indeed, both cyberwar and netwar are modes of conflict that are largely about "knowledge"—about who knows what, when, where, and why, and about how secure a society,

*John Arquilla and David Ronfeldt, *The Advent of Netwar*, MR-789-OSD, 1996, pp. 3–16, 19–24, and 81–82. Some figures and text were omitted for this version.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
1996		**00-00-1996 to 00-00-1996**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Advent of Netwar	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Graduate School of Operational and Information Sciences,Department of Defense Analysis,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
In Athena?s Camp: Preparing for Conflict in the Information Age (John Arquilla and David Ronfeldt eds.). Santa Monica, CA: RAND, 1997

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**19**	

military, or other actor is regarding its knowledge of itself and its adversaries.

The other assumption is that the information revolution favors and strengthens network forms of organization, while making life difficult for hierarchical forms. This implies that conflicts will increasingly be fought by "networks" more than by "hierarchies." Thus, whoever masters the network form should gain major advantages in the new era.

Both assumptions permeate this analysis and are discussed further as it proceeds. A point to emphasize here is that these assumptions affect the entire conflict spectrum. They mean that major alterations are looming in the nature of our adversaries, in the threats they pose, and for the defense measures the United States should consider. Information-age threats are likely to be more diffuse, nonlinear, and multidimensional than industrial-age threats. Cyberwars and netwars may even be mounted at the same time, in mixes that pose uncomfortable societal dilemmas. All this will place the U.S. military and society under increasing pressure to develop new concepts for organization, doctrine, strategy, tactics, and technology.

At present, the U.S. military is the world's leader with regard to thinking, planning, and preparing for cyberwar. The United States is the only country with an array of advanced technologies (e.g., for command, control, communications, and intelligence (C3I), surveillance, stealth, etc.) to make cyberwar an attractive and feasible option. But potential U.S. adversaries have the lead with regard to netwar. Here, the U.S. emphasis must be on defensive measures. This continues a long trend in which the United States has been prepared for waging major wars, while our adversaries may instead wage guerrilla warfare, terrorism, and other irregular modes of conflict. This may be partly the result of displacement—some adversaries, seeing that they should avoid or could not win at regular warfare, have opted for irregular modes, which the U.S. military may then try to treat as "lesser-included cases." Such displacement may occur again with netwar. But, hopefully, netwar will not be perceived as a "lesser-included case" of information-age conflict, for it is not.

Instead of using terms like cyberwar or netwar, many analysts have been treating such points under the rubric of the "revolution in mili-

tary affairs" (RMA). Yet, this very general concept is still mainly about the information revolution and its effects and implications. It led early exponents to view technology innovation as the most important dimension of the RMA. But other, recent exponents have come to accept that the RMA is equally if not mainly about organizational and doctrinal innovation—a view we have emphasized since beginning our efforts to conceptualize cyberwar and netwar. Even so, discussions about the RMA tend to focus on HICs and MRCs that revolve around regular, albeit much-modified military forces. Exponents of the RMA have had less to say about the netwar end of the spectrum (see Arquilla and Ronfeldt, 1995).

The term "netwar" denotes an emerging mode of conflict (and crime) at societal levels, involving measures short of war, in which the protagonists use—indeed, depend on using—network forms of organization, doctrine, strategy, and communication. These protagonists generally consist of dispersed, often small groups who agree to communicate, coordinate, and act in an internetted manner, often without a precise central leadership or headquarters. Decisionmaking may be deliberately decentralized and dispersed.

Thus netwar differs from traditional modes of conflict and crime in which the protagonists prefer to use hierarchical organizations, doctrines, and strategies, as in past efforts to foster large, centralized mass movements along Leninist lines. In short, netwar is about Hamas more than the PLO, Mexico's Zapatistas more than Cuba's Fidelistas, the Christian Identity Movement more than the Ku Klux Klan, the Asian Triads more than the Sicilian Mafia, and Chicago's Gangsta Disciples more than the Al Capone Gang.

Actors across the spectrum of social conflict and crime are evolving in the direction of netwar. This includes familiar adversaries who are modifying their structures and strategies to gain advantage from the rise of network designs: e.g., transnational terrorist groups, black-market proliferators of weapons of mass destruction (WMD), drug and other criminal syndicates, fundamentalist and ethnonationalist movements, intellectual-property pirates, and immigration and refugee smugglers. Some urban gangs, rural militia organizations, and militant single-issue groups in the United States are also developing netwar-like attributes.

But that is not all: The netwar spectrum may increasingly include a new generation of revolutionaries and activists who espouse post-industrial, information-age ideologies that are just now taking shape. In some cases, identities and loyalties may shift from the nation-state to the transnational level of "global civil society." New kinds of actors—e.g., anarchistic and nihilistic leagues of computer-oriented "cyboteurs"—are also beginning to arise who may partake of netwar.

Many if not most netwar actors will be nonstate and even stateless. Some may be agents of a state, but others may turn states into their agents. Odd hybrids and symbioses are likely. Moreover, a netwar actor may be both subnational and transnational in scope.

Many netwar actors may be antagonistic to U.S. interests, such as WMD proliferators. But others, like some transnational social activists, may not. In some cases, a netwar actor may benefit U.S. interests. Many variations are possible. Thus the advent of netwar may prove mainly a bane but at times a boon for U.S. policy.

The full spectrum of netwar proponents may seem broad and odd at first glance. Some actors could be fit into standard notions of LIC, OOTW, and crime. But not all fit easily into prevailing categories. And trying to make them fit risks overlooking the underlying pattern that cuts across all these variations: the use of network forms of organization, doctrine, strategy, and communication attuned to the information age.

Despite the modernity of the concept, historical instances of netwar-like actors abound. Examples mentioned in this study include: irregular warfare in North America during the French and Indian Wars, and the American Revolution in the eighteenth century; the warfare waged by indigenous Spanish guerrillas against the Napoleonic occupation in the early nineteenth century; as well as pirates and other criminals and terrorists that have long operated on the fringes of empires and nation-states. Yet, in contrast to the currently emerging examples of netwar, these early cases were forced, largely by circumstance, into netwar-like designs; these were not designs that were determined by explicit doctrine, or that could be sustained for long, or over great distances.

We think a new term is needed to focus attention on the fact that network-based conflict and crime are increasing. No current terms

about LIC and OOTW fit this purpose. Moreover, the term "information warfare" (IW) and its derivatives (e.g., "infowar," "information warriors") are both too broad and too narrow to be appropriate. On the one hand, IW is used sometimes to refer to the entire spectrum of information-age conflict; on the other hand, it is increasingly associated with narrow technical issues of cyberspace vulnerability, security, and safety.

The term "netwar" connotes that the information revolution is as much about organizational design as about technological prowess, and that this revolution favors whoever masters the network form. The term amounts, then, to both a tool and a prediction:

- *Tool*, because it illuminates—and instructs the eye to focus on—a new but elusive phenomenon requiring new concepts and methodologies to understand: the rise of network forms of organization.
- *Prediction*, because it heralds the prospect that networked adversaries will probably predominate the spectrum of conflict and crime early next century.

The term may strike some readers as fanciful, and a better term may yet be found. But meanwhile, in addition to providing a basis for this analysis, it is already being adopted by protagonists of varied political creeds who believe it resonates with their doctrines and objectives. For example, some extreme rightist militia members in the United States have been heard to declare netwar (or *netkrieg*) against the U.S. government, and have organized a virtual *netwaffe.* Also, center-left activists operating in Mexico sometimes refer to themselves now as "netwarriors."

The phenomenon of netwar is not entirely new—there are examples from decades past—but it is growing and spreading to an extent that will make it quantitatively and qualitatively different from what has gone before. It is becoming both more plentiful and more powerful, enough to compel a rethinking of the overall nature of potential threats, and of the roles and missions for responding to them.

The phenomenon of netwar is still emerging; its organizational, doctrinal, and other dimensions are yet to be fully defined and developed. But the outlines are detectable.

An archetypal netwar actor consists of a web (or network) of dispersed, interconnected "nodes" (or activity centers)—this is its key defining characteristic. It may resemble the bounded "all-channel" type of network. These nodes may be individuals, groups, formal or informal organizations, or parts of groups or organizations. The nodes may be large or small in size, tightly or loosely coupled, and inclusive or exclusive in membership. They may be segmentary or specialized; that is, they may look quite alike and engage in similar activities, or they may undertake a division of labor based on specialization. The boundaries of the network may be sharply defined or blurred in relation to the outside environment.

The organizational structure is quite flat. There is no single central leader or commander; the network as a whole (but not necessarily each node) has little to no hierarchy. There may be multiple leaders. Decisionmaking and operations are decentralized and depend on consultative consensus-building that allows for local initiative and autonomy. The design is both acephalous (headless) and polycephalous (Hydra-headed)—it has no precise heart or head, although not all nodes may be "created equal." In other words, the design is a heterarchy, but also what might be termed a "panarchy" (see below).

The structure may be cellular for purposes of secrecy or substitutability (or interoperability). But the presence of "cells" does not necessarily mean a network exists, or that it is of the "all-channel" design. A hierarchy can also be cellular, as has been the case with some subversive organizations. Or the cells may be arranged in a "chain" or "star" rather than an all-channel shape.

The capacity of this nonhierarchical design for effective performance over time may depend on a powerful doctrine or ideology, or at least a strong set of common interests and objectives, that spans all nodes, and to which the members subscribe in a deep way. Such a doctrine can enable them to be "all of one mind" even if they are dispersed and devoted to different tasks. It can provide an ideational, strategic, and operational centrality that allows for tactical decentralization. It can set boundaries and provide guidelines for decisions and actions so that they do not have to resort to a hierarchy—"they know what they have to do." That is why a nouveau term like panarchy may be more accurate than heterarchy.

The design depends on having a capacity—better yet, a well-developed infrastructure—for the dense communication of functional information. This does not mean that all nodes have to be in constant communication; that may not make sense for a secretive actor. But when communication is needed, information can be disseminated promptly and thoroughly, both within the network and to outside audiences.

In many respects, this archetypal netwar design resembles a "segmented, polycentric, ideologically integrated network" (SPIN). The SPIN concept, identified by anthropologist Luther Gerlach and sociologist Virginia Hine, stems from an analysis of U.S. social movements in the 1960s and 1970s:

> By segmentary I mean that it is cellular, composed of many different groups. . . . By polycentric I mean that it has many different leaders or centers of direction. . . . By networked I mean that the segments and the leaders are integrated into reticulated systems or networks through various structural, personal, and ideological ties. Networks are usually unbounded and expanding. . . . This acronym [SPIN] helps us picture this organization as a fluid, dynamic, expanding one, spinning out into mainstream society (Gerlach, 1987, p. 115, based on Gerlach and Hine, 1970).

The SPIN concept is a precursor of the netwar concept. Indeed, Gerlach and Hine anticipated two decades ago many points about network forms of organization that are just now coming into vogue.

This distinctive design has unique strengths for both offense and defense. On the offense, netwar is adaptable, flexible, and versatile vis-à-vis opportunities and challenges that arise. This may be particularly the case where there is functional differentiation and specialization among the network's nodes. These node-level characteristics, rather than implying a need for rigid command and control of group actions, combine with interoperability to allow for unusual operational flexibility, as well as for a rapidity of maneuver and an economy of force.

When all, or almost all, network elements can perform either specialized or general missions, the mobilization process can unfold rapidly. This capability alone should improve offensive penetration since the defense's potential warning time may be truncated. The

capacity for a "stealthy approach" of the attacking force suggests the possibility that, in netwar, attacks will come in "swarms" rather than in more traditional "waves."[1]

Further, during the course of a netwar offensive, networked forces will, more than likely, be able to maneuver well within the decision-making cycle of more hierarchical opponents. This suggests that other networked formations can reinforce the original assault, swelling it; or they can launch swarm attacks upon other targets, presenting the defense with dilemmas about how best to deploy their own available forces.

In terms of their defensive potential, networks tend to be redundant and diverse, making them robust and quite resilient in the face of adversity. Because of their capacity for interoperability, and their absence of central command and control structures, such network designs can be difficult to crack and defeat as a whole. In particular, they defy counterleadership targeting (i.e., "decapitation"). This severely limits those attacking the network—generally, they can find and confront only portions of it. The rest of the network can continue offensive operations, or swarm to the aid of the threatened nodes, rather like antibodies. Finally, the deniability built into a network affords the possibility that it may simply absorb a number of attacks on distributed nodes, leading the attacker to believe the network has been harmed when, in fact, it remains operationally viable and may actually find new opportunities for tactical surprise.

The difficulty of dealing with netwar actors is deepened when the line between offense and defense is "blurred"—or "blended." When blurring is the case, it may be difficult to distinguish between attacking and defending actions; they may be observationally equivalent. Swarming, for example, may be employed to attack some adversary, or to form an antibody-like defense against incursions into an area that formed part of the network's defensive zone against a hierarchical actor. A historical example is the swarming Indian attack on General George Braddock's forces during the French and Indian Wars—an instance of a network of interconnected American Indian tribes (Gipson, 1946) triumphing over an army designed around a rigid, traditional command hierarchy. While the British saw the Indian attack as presaging a major offensive against the seaboard colonies, it was but an effort to deter incursions into the French-held

Ohio River Valley. The French and their Indian allies, outnumbered by the colonists and British imperial forces, took advantage of the disarray caused by their attack to engage in other pinprick raids. This reinforced the British view of an offensive in the making, compelling them to attend primarily to defensive preparations. This lengthened the time it took for the British to muster forces sufficient for the defense of the colonies and the taking of Canada (Parkman, 1884). Today, as discussed later, the Zapatista struggle in Mexico demonstrates anew the blurring of offense and defense.

The blending of offense and defense will often mix the strategic and tactical levels of operations. An example is the netwar-like guerrilla campaign in Spain during the Napoleonic Wars. Much of the time, the guerrillas, and the small British expeditionary force, pursued a strategic offensive aimed at throwing the French out of Iberia. However, more often than not, pitched battles were fought on the defensive, tactically. Similarly, where the guerrillas were on the defensive strategically, they generally took the tactical offensive. The war of the mujahideen in Afghanistan provides an excellent modern example.

This blurring of offense and defense reflects a broader feature of netwar: It tends to defy and cut across standard spatial boundaries, jurisdictions, and distinctions between state and society, public and private, war and crime, civilian and military, police and military, and legal and illegal. A netwar actor is likely to operate in the cracks and gray areas of a society.

A netwar actor may also confound temporal expectations by opting for an unusual duration and pace of conflict. Thus, it may not be clear when a netwar has started, or how and when it ends. A netwar actor may engage in long cycles of quietly watching and waiting, and then swell and swarm rapidly into action.

Moreover, sometimes it may not be clear who the protagonists are. Their identities may be so blurred, and so tangled with other actors' identities, that it is difficult to ascertain who, if anyone in particular, lies behind a netwar. This may be particularly the case where a network configured for netwar is transnational and able to maneuver adroitly and quietly across increasingly permeable nation-state borders.

This means, as Szafranski (1994, 1995) illuminates in discussing "neo-cortical warfare," that the challenge can be "epistemological": a netwar actor may aim to confound people's most fundamental beliefs about the nature of their society, culture, and government, partly to strike fear but perhaps mainly to disorient people so that they no longer presume to think or act in "normal" terms.

Examples can be found in the behavior of some terrorists and criminals. Terrorists, notably those using internetted, less hierarchical structures (like the "leaderless" Hamas), have been moving away from the use of violence for specific, often state-related purposes, to its use for more generalized purposes. There has been less hostage-taking accompanied by explicit demands, and more terrorist activity that begins with a destructive act aimed at having broad but vague effects. Thus, for example, Islamic fundamentalist Sheik Rahman sought to blow up the World Trade Center with the intent of changing "American foreign policy" toward the Middle East. The current rash of domestic terrorism in the United States—e.g., the bombing in Oklahoma, and the derailment in Arizona—involves violent actions and vague or no demands. This reflects a rationality that disdains pursuing a "proportionate" relationship between ends and means, seeking instead to unhinge a society's perceptions.

Criminals also use methods tantamount to epistemological warfare when they insert themselves deeply into the fabric of their societies, e.g., by wrapping themselves in nationalism, acting like local "Robin Hoods," and/or seeking to influence, if not control, their governments and their foreign and domestic policies. Examples abound, in Colombia, Italy, Mexico, and Russia, where symbiotic ties exist between criminal and governmental organizations.

The more epistemological the challenge, the more it may be confounding from an organizational standpoint. Whose responsibility is it to respond? Whose roles and missions are at stake? Is it a military, police, intelligence, or political matter? The roles and missions of defenders are not easy to define, and this may make both deterrence and defense quite problematic.

Netwar adds to the challenges facing the "nation-state." Its traditional presumptions of sovereignty and authority are linked to a bureaucratic rationality in which issues and problems are categorized

so that specific offices can be charged with taking care of specific problems. In netwar, things are rarely so clear.

It is not easy to make a multiorganizational network function well—a hierarchy is easier to run. A key reason for this is that network forms of organization generally require constant dense communications. The information revolution dramatically enhances the viability of the network form (as discussed below). Thus, the new technologies strengthen the prospects and capabilities for actors to take a netwar approach to conflict and crime.

Indeed, new technologies make possible a rather "pure" variety of netwar in which all strategy and tactics—for example, disinformation campaigns and disruptive computer hacking—occur on "the Net" and in the media. But—and this should always be kept in mind—netwar is not just about the new technologies.

The latest telecommunications systems—including advanced telephone, fax, electronic mail (e-mail), and computerized billboard and conferencing systems—all contribute to netwar, and their roles in recent conflicts are often remarked about. But older technologies, like short-wave radio and cassette tape, are also important for some actors. Computerized desktop publishing, a fairly recent development, enhances the outreach of some actors, but access to traditional print and electronic media remains crucial too, depending on the actor and the audience. Meanwhile, old-style face-to-face meetings, human couriers, and regular mail have not ceased to play roles. If a terrorist or criminal sent a coded fax, this would likely be an example of netwar-related behavior, but if the same actor paid off a journalist for an article critical of some U.S. policy, this may also be an example.

Such technologies enhance the capabilities of a network's members not only to coordinate with each other, but also to collect intelligence on the external environment and on their opponents, and to broadcast or otherwise transmit messages to target audiences. The varieties of netwar actors have used all kinds of old and new, high-tech and low-tech, open and secure, and public and partisan media; indeed, many netwar actors are likely to use a layered mix. The technologies can be used to wage a very public netwar campaign (as in Mexico) or to foster a secretive "virtual conspiracy" (as may be an aim of some extreme rightists in the United States).[2]

THE RISE OF NETWORK FORMS OF ORGANIZATION

Anthropologists and sociologists have studied *social* networks for many decades. According to the most established school of thinking, basically all social organizations—families, groups, elites, institutions, markets, etc.—are embedded in networks of social relations (Granovetter, 1985; Nohria and Eccles, 1992). For this school, the network is more the "mother of all forms" than a specific type of complex organization.

Prior to the 1990s, scholarly writings occasionally appeared that treated the network as a specific, deliberate, even formal *organizational* design (e.g., Heclo, 1978; Perrow, 1979; Chisholm, 1989; also Gerlach and Hine, 1970; Gerlach, 1987). But such efforts were more the exception than the rule, and some occurred on the margins of the social sciences, including the illuminating work by Gerlach and Hine on SPINs that we quoted earlier.

Lately, and largely as a result of research by economic sociologists who study innovative corporate designs (notably Powell, 1990; and Powell and Smith-Doerr, 1994), a new school of thinking about networks is beginning to cohere. It looks beyond informal social networks to see that formal organizational networks are gaining strength as a distinct design—distinct in particular from the "hierarchies and markets" that organizational economists and economic sociologists normally emphasize:

> [T]he familiar market-hierarchy continuum does not do justice to the notion of network forms of organization. . . . [S]uch an arrangement is neither a market transaction nor a hierarchical governance structure, but a separate, different mode of exchange, one with its own logic, a network (Powell, 1990, pp. 296, 301).

This new school of analysis and the numerous examples and case studies it affords serve to validate our point that network forms of organization are on the rise and becoming more viable than ever. But the new school is mostly about economic organization. And clear, precise definitions are still lacking as to what is and is not a network.

Distinctions may be made among what are termed "chain," "star" or "hub," and "all-channel" types of networks. We focus on the all-channel type, in which all members are connected to each other and

do not have to go through other members (as in a chain or hub design) to communicate and coordinate with each other.

Despite the claims of some anthropologists and sociologists about the significance of the *social* networks they study for all manner of personal and institutional behaviors, the network as a formal *organizational* design has generally had poor standing among many economists and theorists (e.g., Williamson, 1975). Networks have long been deemed inefficient and inferior as a form of organization, especially compared with hierarchies and markets. Among other things, networks were said to require too much back-and-forth, to require "high bandwidth" communication among all members, to take too long to reach decisions, and to be too vulnerable to free riders.

Indeed, all-channel networks do require rapid, dense, multidirectional communications to function well and endure—more so than do other forms of organization. The past limitations of this form of organization are closely tied to information and communications factors.

The new technologies—e.g., advanced telephone, fax, e-mail, computer billboard, and conferencing systems, supported by fiber-optic cable and satellite systems—finally provide the level of connectivity and bandwidth that favors all-channel organizational designs. Today, diverse, dispersed, autonomous actors are able to consult, coordinate, and act jointly across great distances on the basis of more, better, and faster information than ever before. The rise of the network form thus reflects, and is tied to, the information revolution.

The rise of network forms of organization is at an early stage, still gaining impetus. It may be decades before this trend reaches maturity. But it is already affecting all major realms of society. In the realm of the *state*, it is facilitating the development of interagency mechanisms for addressing complex policy issues that cut across jurisdictional boundaries. In the realm of the *market*, it has been facilitating the growth of *keiretsus* and other distributed, web-like global enterprises (and so-called "virtual corporations"). Indeed, volumes are being written about the benefits of network designs for business corporations and market operations—to the point that casual (and

some not-so-casual) observers might presume that this is the realm most affected and benefited.

Yet, actors in the realm of *civil society* may be the main beneficiaries. The trend is increasingly prominent in this realm, where issue-oriented multiorganizational networks continue to multiply among activists and interest groups across the political spectrum. Over the long run, civil society is likely to be strengthened more than the other realms, in both absolute and relative terms.

What is meant by "civil society"—never a clear term—continues to evolve. Classic views, starting centuries ago, have emphasized "associations" that mediate between state and society within a nation: e.g., churches, schools, labor unions, businesses, political parties, and other voluntary groups, interest groups, professional organizations, etc. Recent views, beginning a few decades ago, do not reject the classic views but emphasize "new social movements"—such as environmental, human-rights, peace, and other movements—that are increasingly transnational in scope. Two rising indicators—listings in the *International Directory of Non-Governmental Organizations* (published since the 1970s), and subscribers to the computer networks affiliated with the Association for Progressive Communications (APC, the favored network of networks for activists since its formation in 1989)—speak to the rising importance of nongovernmental organizations (NGOs) for policy issues around the world, and the relationship between the NGOs' rise and the information revolution.

Even where civil society has been strong—as in the liberal democracies of Western Europe and North America—it has long been characterized by groups that often had to work in isolation or in fleeting coalitions and that, as a result, were weaker than state and market actors. Now, however, the new information technologies and related organizational innovations increasingly enable civil-society actors to reduce their isolation, build far-flung networks within and across national boundaries, and connect and coordinate for collective action as never before. As this trend deepens and spreads, it will strengthen the power of civil-society actors relative to state and market actors around the globe (Frederick, 1993; Ronfeldt, 1993).

For years, a cutting edge of this trend could be found among left-leaning activist NGOs concerned with human-rights, environmental, peace, and other social issues at local, national, and global levels. Many of these rely on APC affiliates for communications and aim to construct a "global civil society" strong enough to counter the roles of state and market actors. In addition, the trend is spreading across the political spectrum. Activists on the right—from moderately conservative religious groups, to militant antiabortion groups—are also building national and transnational networks based in part on the use of new communications systems.

Not only civil society but also "uncivil society" is benefiting from the rise of network forms of organization. Uncivil actors—like criminal gangs and terrorist groups—once operated pretty much in isolation from each other. Now, transnational criminal organizations (TCOs) are taking shape (Williams, 1994, 1995). What might be termed transnational revolutionary organizations (TROs) are also emerging on the political left (e.g., Hamas) and the right (e.g., among white supremacy groups). All are building global networks as "force multipliers," and using all manner of new communications technologies to do so.

This trend—the rise of network forms of organization—is still at an early stage, but it is already a very important topic for theoretical research and policy analysis. New and interesting work can be done just by focusing on this trend. At the same time, the trend is so strong that, projected into the future, it augurs transformations in how societies are organized—if not societies as a whole, then at least key parts of their governments, economies, and especially their civil societies.

The trend thus raises questions not only about the significance of the network form itself, but also relative to other forms of organization. The rise of the network form should be analyzed partly in terms of how it is interwoven with, and related to, other basic forms of societal organization.

CHALLENGES FOR U.S. POLICY AND ORGANIZATION

This research on the looming challenge of netwar continues to bear out a set of propositions that we identified some time ago about the

information revolution and its likely implications (Arquilla and Ronfeldt, 1993):

The information revolution favors and strengthens networks, while it erodes hierarchies. The continued explosive growth of political, business, social, and other networks that benefit societies, as well as of criminal, terrorist, and other networks that threaten them confirm this proposition, as does the concomitant "softening" of traditional statist institutions.

Hierarchies have a difficult time fighting networks. Examples of this appear across the conflict spectrum. Some of the best may be found in the generally failing efforts of many governments to deal with TCOs. The persistence of religious revivalist movements, as in Algeria, often in the face of unremitting statist opposition, shows the robustness of the network form, on defense and offense. The Zapatista movement in Mexico, with its legions of supporters and sympathizers among local and transnational NGOs, shows that social netwar can put a democratizing autocracy on the defensive and pressure it to continue adopting reforms.

It takes networks to fight networks. The case of the Southeast Asian pirates makes this point well. The first effort to cope with the resurgence of piracy was state-centered and failed miserably. The establishment of a transnational counter-piracy network proved successful in a relatively short time. This proposition may well be analogous to others in military doctrine, particularly that "it takes a tank to fight a tank."

Whoever masters the network form first and best will gain major advantages. In these early years of the information age, those adversaries who have advanced at networking (e.g., criminals, terrorists, and activists) are enjoying a marked increase in their power relative to state agencies. While networking once allowed them simply to keep from being eradicated, it now allows them to compete on more nearly equal terms with states and with other hierarchically oriented adversaries. The history of Hamas and that of the Cali cartel illustrate this.

The information revolution is about both technology and organization. While technology innovation is revitalizing the network form, one must not ignore the importance of organizational innovation.

Indeed, every information revolution has involved an interplay between technology and organization that affects who wins and loses. For example, a millennium before the printing revolution, the early Catholic Church had a networked organization that confronted and overcame brutal opposition from one of history's most successful hierarchies, the Roman Empire. The Church later developed its own great hierarchies, ironically making it susceptible to dissent as the printing revolution emerged in the 16th century.

Today, those who want to defend against netwar will, increasingly, have to adopt weapons, strategies, and organizational designs like those of their adversaries. This does not mean mirroring the adversary, but rather learning to draw on the same design principles that he has already learned about the rise of network forms in the information age. These principles depend to some extent upon technological breakthroughs, but mainly on a willingness to innovate organizationally.

For U.S. policy, an early implication of our work is that counternetwar will require very effective interagency operations, which by their very nature involve networked structures. It should not be necessary, or desirable, to replace all hierarchies with networks. Rather, the challenge will be to blend these two forms skillfully, while retaining enough central authority to encourage and enforce adherence to truly networked processes. In this manner, states may come to be better prepared to confront the multitude of new threats emerging in this information age.

REFERENCES

Arquilla, John, and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy,* Vol. 12, No. 2, pp. 141–165 (Summer 1993).

———, "(Book Review) Welcome to the Revolution . . . in Military Affairs," *Comparative Strategy,* Vol. 14, No. 2, pp. 331–341 (Spring 1995).

Chisholm, Donald, *Coordination Without Hierarchy: Informal Structures in Multi-organizational Systems,* Berkeley: University of California Press, 1989.

Frederick, Howard, "Computer Networks and the Emergence of Global Civil Society," Linda M. Harasim (ed.), *Global Networks: Computers and International Communication*, Cambridge, Mass.: The MIT Press, 1993, pp. 283–295.

Gerlach, Luther P., "Protest Movements and the Construction of Risk," B. B. Johnson and V. T. Covello (eds.), *The Social and Cultural Construction of Risk*, Boston: D. Reidel Pub. Co., 1987, pp. 103–145.

Gerlach, Luther P., and Virginia Hine, *People, Power, Change: Movements of Social Transformation*, New York: The Bobbs-Merrill Co., Inc., 1970.

Gipson, Lawrence H., *The Great War for Empire: The Years of Defeat*, New York: Alfred A. Knopf, 1946.

Granovetter, Mark S., "Economic Action and Social Structure: The Problem of Embeddedness," *American Journal of Sociology*, Vol. 91, No. 3, November 1985, pp. 481–510.

Heclo, Hugh, "Issue Networks and the Executive Establishment," Anthony King (ed.), *The New American Political System*, Washington, D.C.: The American Enterprise Institute, 1978, pp. 87–124.

Kelly, Kevin, *Out of Control: The Rise of Neo-Biological Civilization*, New York: Addison-Wesley Publishing Company, 1994.

Nohria, Nitin, and Robert G. Eccles (eds.), *Networks and Organizations: Structure, Form, and Action*, Boston, Mass.: Harvard Business School Press, 1992.

Parkman, Francis, *Montcalm and Wolfe: The Decline and Fall of the French Empire in North America*, New York: Collier, 1884; reprinted 1962.

Perrow, Charles, *Complex Organizations: A Critical Essay*, 2nd Edition, Glenview, Ill.: Scott, Foresman and Company, 1979.

Powell, Walter W., "Neither Market Nor Hierarchy: Network Forms of Organization," Barry M. Staw and L. L. Cummings, ed., *Research in Organizational Behavior: An Annual Series of Analytical Essays*

and Critical Reviews, Vol. 12, Greenwich, Conn.: JAI Press Inc., 1990, pp. 295–336.

Powell, Walter W., and Laurel Smith-Doerr, "Networks and Economic Life," Neil J. Smelser and Richard Swedberg, eds., *The Handbook of Economic Sociology*, Princeton, N.J.: Princeton University Press & Russell Sage Foundation, 1994, pp. 368–402 (Chapter 15).

Ronfeldt, David, *Institutions, Markets, and Networks: A Framework About the Evolution of Societies*, Santa Monica, Calif.: RAND, DRU-590-FF, December 1993.

Szafranski, Colonel Richard, "Neo-Cortical Warfare? The Acme of Skill," *Military Review*, November 1994, pp. 41–55.

———, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal*, Spring 1995, pp. 56–65.

Van Creveld, Martin, *The Transformation of War*, New York: Free Press, 1991.

Williams, Phil, "Transnational Criminal Organizations and International Security," *Survival*, Vol. 36, No. 1, Spring 1994, pp. 96–113.

———, "Transnational Criminal Organizations: Strategic Alliances," *The Washington Quarterly*, Vol. 18, No. 1, Winter 1995, pp. 57–72.

Williamson, Oliver E., *Markets and Hierarchies: Analysis and Antitrust Implications*, New York: The Free Press, 1975.

NOTES

[1]Swarm networks and the capacity of networks for swarming are raised by Kelly (1994).

[2]Credit for the term "virtual conspiracy" is owed to journalist Lou Dolinar of *Newsday*.